[Mission Acronym] FSW Sustaining Engineering Plan

Flight Software Branch – Code 582

[Template] Version 1.0 – 08/17/05

582-2005-001

Goddard Space Flight Center
Greenbelt, Maryland

National Aeronautics and
Space Administration

FORWARD

This document is a skeleton Sustaining Engineering Plan intended for use by Code 582 (Flight Software Branch) personnel as the basis for a mission-specific Flight Software Sustaining Engineering Plan.

The following style conventions are used throughout:

Text in this style (style name “Body”) is used for text that is equally applicable to all plans and should be included in the plan without modification. All document section headings are in the same category (although their style names vary depending on outline level).

[Text in this style (style name “TAILORING ADVICE”) is advice on how to tailor the text in any specific section.]

As the plan is developed, the generic [TAILORING ADVICE] text should be replaced with material that applies to the specific project.

GENERAL TAILORING GUIDELINES

This section includes general tailoring guidelines applicable to the whole document. Specific recommendations are included in applicable sections.

All components of the table of contents should be addressed, but the level of detail is left up to the Team based on flight software complexity and customer needs/expectations. The length and level of detail of the plan should be commensurate with the scope and complexity of the project. Section headings may be added where necessary, but existing headings should not be modified or deleted. If a particular section is not applicable to the specific plan under production, that fact should be noted under the section heading, together with a brief explanation.

In the target Plan, this entire section (“Forward”) can be removed.

PLAN UPDATE HISTORY

[This table shows the update history for the Template. For plans developed using this template, the elements of this table should be replaced with mission-specific plan update information.]

Version	Date	Description	Affected Pages
0.90	01/13/05	Initial version	All
0.91	06/17/05	Rewrites of sections 2 and 5, and Revisions to 3.0, 4.0, 6.1, 6.2, 6.4, 7.1, 8.1.1, 8.1.2, and 8.1.4, 9	2 - 13
1.0	08/17/05	Revisions to 2.2, 4.0, 5.0, 8.0 (also moved as sec 6), 7.0 (parts incorporated into section 5, the rest deleted), and Appendices A, C, & D	All

CONTENTS

1.0 FSW SUSTAINING ENGINEERING CHARTER

The FSW Sustaining Engineering Team (FSSE) will provide the technical expertise and proven processes to directly sustain the continuing effectiveness of the [mission or instrument] on-orbit FSW. The FSSE will develop modifications to the FSW to respond to onboard hardware issues, satisfy science needs, and improve flight operations. The team will further support flight operations, science personnel, project engineers and management in the analysis, recovery, and resolution of spacecraft anomalies. The FSSE will also respond to FSW-related inquiries and will investigate FSW issues as directed. Within the context of these roles, sustaining engineers will develop insight into the spacecraft system as a whole and how the subsystems relate to the FSW. The items discussed in this plan directly support these goals and describe the controls necessary to maintain the integrity of the [mission or instrument] FSW.

2.0 PROJECT INTERFACE

FSW development and preparations for on-orbit maintenance activities are accomplished under the authority of the [mission or instrument] Project. Actual on-orbit FSW maintenance occurs under the authority of the [mission or instrument] Operations [and Science] Project[s].

2.1 FSW SUSTAINING ENGINEERING MEMORANDUM OF AGREEMENT

The Flight Software Branch/Code 582 (FSB) will develop a FSW Sustaining Engineering Memorandum of Agreement (MOA) with the [mission or instrument] Project. This agreement establishes the commitment between the Project and the FSB for long term FSW sustaining engineering under the leadership of the FSB. This agreement provides a yearly funding estimate plus roles and responsibilities both prior to launch and for the on-orbit design life of the mission. It also specifies the Testbed and tools required from the Project for accomplishing FSW maintenance.

2.2 OFFICIAL START OF THE SUSTAINING ENGINEERING PHASE

The nominal transition of primary FSW responsibilities to the FSSE will occur following successful completion of In-orbit Check-out (IOC) of the [mission or instrument]. As of the date this document was signed, this transition will take place approximately [month, data, year]. [If earlier transition of some/all of the FSW has been agreed to, enter the actual agreement here. It is not unusual for maintenance staff to take over some/all FSW roles prior to launch while under the clear leadership of the development team. This early transition greatly facilitates seamless transition of the sustaining engineering responsibilities to the FSSE staff.]

Following IOC, the FSSE will be funded and directed via the [mission or instrument] Operations [and Science] Project[s].

2.3 TRANSITION OF FSW RESPONSIBILITIES TO THE FSSE

A FSW Transition Plan, from the FSW development team [specify who that team works for] to the FSSE under the FSB, will be developed. The FSW Transition Plan is defined in subsection [x.x] of this document and will be approved by both the [mission or instrument] Project (development) and the [mission or instrument] Operations Project.

2.4 FSW-TO-OPERATIONS AGREEMENT

A [mission or instrument] FSW-to-Operations Agreement (OA) will be developed by the FSB to allocate specific responsibilities and commitments between the Flight Operations Team (FOT) and the FSSE. This will include FSSE support related to on-orbit anomaly investigations, FOT responsibilities when an anomaly occurs, responsibilities to the FSW Configuration Control Board, FSSE and FOT roles related to FSW and onboard table and command changes , maintenance and interface responsibilities concerning FSW products (patch loads, ground reference images, FSW archives, mission operations tools), and Mission Operations Center (MOC) access to the FSW Testbed. The [mission or instrument] OA itemizes and clarifies the responsibilities between the FOT and FSSE with a focus on minimizing risks that might otherwise result from ineffective communications and change in personnel. [Note that if other organizations in addition to the FOT share operating responsibilities with the FSSE relating to FSSE-maintained FSW (for example maintainers of other areas of the mission or instrument FSW, or developers who retain a role relating to FSSE-maintained software), then the operational interface requirements between them and the FSSE are also delineated in the OA].

2.5 FSW CONFIGURATION CONTROL BOARD

The FSB will establish a [mission or instrument] on-orbit FSW Configuration Control Board (CCB), which will formally begin with the end of IOC and remain active for the life of the [mission or instrument]. The board will be co-chaired by the FSB Sustaining Engineering Lead and the [Mission Director or Principal Investigator]. All work performed by the FSSE must be approved, tracked, and directed through the FSW CCB, with meetings nominally occurring once per month. Changes to all configured items, including [mission or instrument] FSW, simulators, databases, ground systems, and Testbed hardware, will be documented and monitored via Configuration Change Requests (CCRs). All other FSW support work, including anomaly support, FSW investigations, support for science events, and Testbed maintenance, shall be documented and tracked via Work Requests (WRs).

3.0 APPLICABLE DOCUMENTS

FSW Patch Development Process

"FSW-202 Patches" will be used by the FSSE.

[If the above procedure will not be used, cite the one that will.]

CM Plans and procedures

[A configuration management plan must be cited. Replace the above text with the actual name of the process.]

Memoranda of Agreement

[A Memorandum of Agreement must be cited. Replace the above text with the actual name of the process.]

Operations Agreements

[An operations agreement must be cited. Replace the above text with the actual name of the document.]

[List any interface control documents that will be applicable.]

FSB Testbed Move and Recertification Plan [a lab move and recertification procedure must be cited here if the lab is to be moved.]

[A procedure for archiving the FSW and all supporting software must be cited.]

4.0 FSW OVERVIEW

This section will describe the FSW that will be governed by this plan.

What follows is a brief overview of the [mission or instrument] FSW subsystem.

[Give a brief overview of the FSW here.]

Refer to the following user's guides and requirements documents for more information.

[List all the FSW user's guides and requirements documents here.]

3.0 FSW Data Configuration

The FSW data and configuration are changeable via tables and commands. All tables and all data or configuration changing commands are critical and may not be uplinked without the consent of the FSSE. Otherwise the on-board FSW will diverge from the ground image, risking the integrity of future analyses and FSW changes. The following is a list of the data or configuration changing commands.

[List the commands that cause a change to FSW data or configuration.]

[E.g. The Swift /BAT FSW contains parameters changeable only by command that affect the way the FSW processes the science data. If these parameters were changed without notifying the FSSE, the on-board FSW would diverge from the ground image risking the integrity of future analyses and FSW changes.]

3.0 Non-volatile Memory

The [XXXX Mission] FSW processor contains two copies of EEPROM. The first copy will not be modifiable on orbit. FSSE engineers will be able to write to the second copy on orbit.

[E.g. ICESat/GLAS has two copies of EEPROM, one copy is modifiable in flight and the other is used as a backup. WMAP has the same memory configuration as ICESat/GLAS, but neither copy is allowed to be modified.]

3.0 Volatile Memory

The [XXXX Mission] FSW processor contains RAM, DRAM, & SRAM. Addressing is dynamically allocated. The following table contains details regarding the architecture of the FSW.

[E.g. Swift/BAT FSW addressing is dynamically allocated. This affects the methods used for patching.]

[Complete the following table, expanding it to include all types of RAM and ROM present on the given mission.]

FSW Processors	Function	Language	OS	Memory Type & Size	Non-Volatile Size	Lines of Code

3.0 FSW Workarounds During the Sustaining Engineering Phase

The FSW contains the following “features” that require workarounds during the Sustaining Engineering Phase. The workarounds are also listed below.

[E.g. The RXTE FSW will initiate a WARM restart if, at the time the checksum task is suspended, it is processing a code segment area that is then patched. To work around this “feature”, the RXTE Sustaining Engineering Team must understand what segments they will modify with each patch and monitor the checksum processing in order to suspend it when it is not in the region to be patched.]

3.0 Contact Length

The [XXXX Mission] will communicate with the ground via [TDRS, Ground Stations, DSN, etc.] [give the frequency for each contact method here: once a day, once an orbit, etc.]. Each nominal contact will be approximately [give the contact length here]. The nominal method of patching the FSW is expected to be [give the nominal patch method here]. The largest of these patches could be [size] bytes. At the nominal uplink rate of [give the uplink rate here, factoring in communication lag time], it will take [period of time] to load the largest patch. [Period of time] of each pass will be used by the FOT for routine operations. Therefore, [number of contacts] contacts will be required. The largest system table is [size] bytes. At the nominal uplink rate of [give the uplink rate here, factoring in communication lag time], it will take [period of time] to load this table. Therefore, [number of contacts] contacts will be required.

[For example, the Swift/BAT mission’s nominal patch method is task replacement. Given the largest task, the nominal uplink rate, and the contact length of ~10min, at least eight contacts are needed to load this task. If the whole RAM image needed to be replaced via orbital ground contacts, via orbital ground contact, 60 contacts would be required unless TDRSS contacts can be scheduled. In another example, ICESat/GLAS has a set of 360 related tables. During the mission, the scientists needed to update all of them at once. This necessitated 360 consecutive table loads. Give the average ground contact time of 10min, and the uplink rate with ground-to-ICESat and ICESat-to-GLAS communication lag times factored in, 51 contacts were required.]

[This analysis of contact length is done in order to flesh out any risks, restrictions, or workarounds necessary.]

5.0 FSW SUSTAINING ENGINEERING RESPONSIBILITIES

5.1 Pre-Launch

5.1.1 FSW Sustaining Engineering Preparedness

The FSW Launch Preparations Checklist in Appendix A accounts for all FSSE activities, as further described below, that the FSSE will undertake to prepare for the Sustaining Engineering (SE) phase. In order to evaluate and implement the checklist activities, a series of monthly meetings will be held beginning one year before the anticipated launch date of [expected launch date]. The meetings will continue until the checklist, and associated SE readiness, is completed. The meeting attendees will include the post-launch [mission or instrument] FSW CCB Chair and FSSE engineers. Others to be consulted as needed to clarify SE issues include the [mission or instrument] FSW development engineers, the Flight Operations Team, science personnel, and FSB facilities staff.

5.1.2 Use of Heritage FSW and Related Products

The [mission or instrument] FSW claims its heritage from the [missions or instruments. Indicate here what experience the FSSE may have with similar FSW and what benefits the team will glean from reuse, etc]. The FSW Development, Test and Mission Operations Tools Set is derived from [similarly name any heritage ties and benefits therein]. The Testbed environment is similar to [again cite any like spacecraft testbeds from the past and related benefits. Further indicate any past similarities or reuse of hardware or software pertaining to the SE role].

5.1.3 FSSE Roles

The FSSE provides personnel to manage the wide range of team responsibilities described in this section. These roles may be distributed across the team or, in the case of limited manpower resources, one person may perform multiple roles. The lead FSW engineer is responsible for assigning work to all FSW engineers and interfacing with [mission or instrument] personnel (mission director, CCB Chair, FOT members, the principle investigator and other science staff, etc). The FSW engineers perform all technical FSW work, including performing the FSW life-cycle change process, Flight Operations support, Testbed management and use, and software tools maintenance and use. The Quality Assurance engineer ensures that all SE processes are followed. The Testbed Manager oversees all Testbed usage and configuration changes, and supports the servicing and repairing of Testbed hardware. The Configuration Manager ensures that all changes to FSSE-managed software and hardware are properly controlled, including saving and protecting all system changes. The Librarian manages all hardcopy and electronic documentation and archiving.

5.1.4 FSSE Training

The FSSE will develop insight into the [mission or instrument] FSW through review of the software and related FSW documentation, including [list the known specific documents such as requirements, design, algorithms, user's guides, test plans, etc]. FSSE team members will be assigned specific areas of the [mission or instrument] FSW for the purpose of familiarizing themselves with each area, developing tutorial presentations, and delivering those presentations to the rest of the team. The tutorials will include discussions relating to on-orbit operational use and maintenance, including table and command interfaces and change methodology.

[Reference here whether sustaining engineers have been part of the development and/or test phases, and how that role, as "on-the-job" training, will support preparedness for the FSW SE role.]

The FSSE will also become familiar with the Testbed environment, including developing, performing, and certifying patch procedure exercises so that the entire patch process is well understood and in place for on-orbit sustaining engineering. FSW tools and procedures shall be studied and exercised, including [list tools, such as ones for patch development and test, FSW analysis, operations interface, etc, and existing procedures for bringing up the Testbed, running acceptance tests, etc].

5.1.5 Software Configuration Management

The [mission or instrument] post-launch FSW Configuration Management (CM) will be detailed in the [cite the plan], as described in Appendix B. The plan deslineates the CM software process and the work instructions for configuring all software before launch, including the FSW, simulators, tools, test procedures and results, and other Testbed elements. [Indicate whether the CM method is being assumed from the developer's approach, or if applicable what issues may exist in any transition to a different CM methodology.]

5.1.6 FSW Documentation and Tools Development

The FSSE will gather all documents, procedures, and software tools received from the [mission or instrument] FSW development team, and then identify, develop and/or enhance them as needed to perform the [mission or instrument] FSW SE role.

The [mission or instrument] FSW development team is expected to deliver the following FSW documentation to the FSSE: [name and describe this inherited documentation set]. Candidate documents for review and further development include [name and describe the specific documents pertaining to FSW requirements, design, algorithms, test plans, users' guides, version description, the operations agreement, etc]. The FSSE will electronically catalog the documents through [describe the on-line system of cataloging documents for the project if there is one and if it will be available through the life of the mission.] FSThe hardcopy document library will be organized and located [provide details].

The [mission or instrument] FSW development team is expected to deliver the following development environment tools to the FSSE: [name and describe this inherited tools set]. Additional software tools and enhancements include: [name and describe each one, including when and how these tools will be developed. Use the tools table in Appendix A to help determine the additional tools].

5.1.7 FSW Regression Test Set

The FSSE shall develop a Regression Test set for post-launch patch testing [clarify if this test suite has an existing starting point such as the developer's suite of acceptance tests]. The need for expanded software tools in the Testbed for anomaly analysis, patch development and test, and science or operations interface support, shall be examined and reconciled.

5.1.8 Test Bed [Construction,] Move and Certification

The origination of the FSW SE Testbed, as described in Section 6, will be the [name source of Testbed, for example developer's development Testbed, a new Testbed to be constructed by the developer, etc]. The FSSE will work with the [mission or instrument] Project, the FSW development team [specify who that team works for], and FSB facilities staff to ensure the move and recertification of the Testbed to [give exact location]. The move and recertification shall be governed by the guidelines in the FSB Testbed Move and Recertification Checklists [or name another document if applicable]. The Testbed will be moved [specify time of move and any clarifying information, for example, to coincide with spacecraft ship when Testbed usage will be low] and be fully recertified by [specify time].

5.1.9 Launch Simulations Support

The FSSE will participate in pre-launch mission simulations, including [list the planned simulations, such as launch and early orbit checkout activities, science maneuvers, orbit adjustments, end-to-end tests, etc]. Support will include conferring on FSW maintenance scenarios, developing anomaly simulations, preparing loads, and providing FSW-related analysis and support during the simulations.

5.1.10 Support for [Mission or Instrument] Reviews and Operational Readiness

The FSSE will ensure the FSW operational readiness of the [mission MOC and/or instrument SOC] and will support the [mission or instrument] operational readiness review. [Indicate also whether the FSSE will support other pre-launch reviews relative to the SE capability, including reviews for FSW development, instrument readiness, ground system, etc.]

5.2 Launch and Post-Launch

5.2.1 [Mission or Instrument] FSW CCB Support

All FSW post-launch support will be governed via the [mission or instrument] FSW CCB (see section 2.5). The FSSE will support the CCB meetings to report and discuss status with the CCB Chair(s) and CCB members, and to agree upon dispositions and priorities of all FSW work. All such work will be documented in the online [mission or instrument] FSW CCR/WR database as either a Configuration Change Request (CCR) or a Work Request (WR, see section 9.1). As the primary implementers of all CCRs and ERs, FSSE personnel will ensure that all CCRs and WRs are kept up to date. The [mission or instrument] FSW CCR/WR database will be accessible via the FSB web site at ([insert URL]).

5.2.2 Launch and In-Orbit Checkout (IOC) Support

The FSSE will support the FSW developer and [mission FOT and/or instrument SOC] concerning FSW functionality and on-orbit FSW issues during launch and IOC. This active role will provide the FSSE with valuable FSW training and insight into FSW behavior onboard before the final transition of primary SE responsibility to the FSSE. [Discuss the specific FSSE roles during this period just before official handover of all FSW SE duties to the FSSE. Include whether the FSSE will have a presence and role in the MOC or SOC, for example providing 24/7 shift support for two weeks, etc. Also describe any FSSE work to be provided for anomaly investigations, patch development & test, and other areas in support of the FSW developer, FOT, or science community].

5.2.3 FSW-related Support to the [Mission FOT or Instrument SOC]

The FSSE will investigate FSW operations issues and answer related questions on functionality of the code, flight hardware and/or software interfaces, ground commands to the FSW, telemetry, and operational scenarios. The FSSE will examine [FOT or SOC-requested] FSW options and provide FSW-related training as needed to [FOT or SOC] personnel.

The FSSE will provide Testbed set up and support to validate flight operations procedures, including checkout of planned onboard scenarios and control center FSW or hardware configuration changes. The team will also support [FOT or SOC] training exercises as requested.

The FSSE will provide FSW products to the [FOT or SOC], including FSW loads, updated FSW documentation, database updates, FSW ground reference images, etc.

5.2.4 On-Orbit Anomaly Investigation / Project Engineering and Management Support

The FSSE will provide [mission or instrument] FSW-related analysis of spacecraft or instrument anomalies. [Discuss the Sustaining Engineers' availability to respond to anomalies 24/7]. The investigation process is provided in Appendix C [note: Appendix C is an example which could be fine tuned for this mission]. FSSE engineers will support the understanding of the anomaly through examination of FSW-reported status in real-time and playback telemetry, memory dumps, ground command sequences, etc. The FSSE will confirm FSW responses and re-create the anomaly in the Testbed as needed to characterize the cause of the anomaly. The team will also participate in anomaly review meetings and review boards, as requested.

The FSSE will support the recovery from spacecraft emergencies by validating proposed recovery solutions in the Testbed and aiding the development and execution of spacecraft reconfiguration procedures. The team will verify the proper onboard functioning of the [mission or instrument] FSW following on-orbit recovery.

FSSE engineers will support questions and requests from project engineers and management, perform further analysis with other subsystem specialists, and recommend, develop, test, and deliver FSW solutions to avoid or react to similar anomalies in the future.

5.2.5 FSW Change Development

The [mission or instrument] FSW Patch Development Process is described in [cite the patch development process that will be used]. The FSSE will develop, fully test and document approved FSW patches and FSSE-controlled table changes (as defined in the [site the exact name of the Operations Agreement]). FSSE engineers will analyze the feasibility, work effort, and benefits of each proposed FSW change. Approved changes will be technically managed through formal reviews (some of which may be combined for efficiency), for Requirements, Design, Code Walkthrough, Test Plan, Test Results, and Uplink Readiness.

FSSE engineers will support the uplink of FSW patches, including providing the installation procedure [clarify the procedure that the FSSE will use to verify that the contents of the file received by the MOC match the files that were sent]. A final uplink verification will be performed by [cite the method, including whether a MOC-to-Testbed test can be performed with the exact uplink procedure and if not, what specific steps will be taken to ensure the successful uplink of the FSW change]. The team will support the coordination of uplink activities to ensure proper ground/flight interfaces. Following the loading of the FSW change, the FSSE will verify that the FSW is functioning as expected.

The FSSE will develop and deliver a Patch Delivery Summary (see Appendix D) to document and closeout each CCR. [If a different documentation template or process is used, cite that method here instead]. The FSSE will archive each change with all related software and will also provide any FSW image updates or related products to other test or operations facilities as required to ensure that these facilities stay in step with the latest FSW changes.

5.2.6 FSW Development and Test Environment Maintenance

The FSSE will be responsible for controlling and maintaining or overseeing the maintenance (in the case of the hardware) of the [mission or instrument] FSW Testbed (see Section 6). This entails ensuring the proper functioning of the Testbed at all times, including maintenance of commercial and special hardware, systems management, computer operations, and configuration management of the software development environment.

5.2.7 Maintenance of Software Used for FSW Sustaining Engineering

The FSSE will ensure the completeness of the [mission or instrument] FSW Development, Test and Mission Operations Tools Set, developing enhancements as necessary to test and analyze FSW changes, support interface changes between the MOC and Testbed, and improve visibility into FSW characteristics. [Include here references to any mission-specific special software tools or packages that the FSSE will maintain. If ACS FSW is being maintained, reference the maintenance role concerning the dynamic simulator, for example indicating that the FSSE will improve dynamic modeling of the flight hardware performance and on-orbit spacecraft environment as necessary for closed loop attitude control, command and data handling, and other interfaces and onboard functions.]

5.2.9 Retention of FSW Expertise

The FSSE will ensure the availability of [mission or instrument] FSW maintenance specialists for commitment to mission needs as required, including the depth of expertise to respond to increased manpower needs or loss of personnel. [Indicate any specifics on how knowledge pertaining to the FSW sustaining engineering phase will be retained by the group, for example, resolving to have access to at least two knowledgeable engineers at all times.] Continued civil servant and contractor FSW expertise will also be assured for special support concerning operations characteristics, anomaly investigating and safing recovery techniques, the FSW test environment, test cases, the test process, and test results for nominal and contingency flight situations.

6.0 FSW SUSTAINING ENGINEERING INFRASTRUCTURE

6.1 FSW TESTBED (FSTB) LOCATION

The testbed is currently located in [testbed location] and will be located in [testbed location] for the sustaining engineering phase. [Describe how the facility is and will be secured.] The testbed will have a command/telemetry connection to the control center.

6.1 FSTB COMPONENTS

[List each component (simulators, power supplies, ETUs, diagnostic equipment, bus monitors, etc.) needed for the test bed. This list should be developed early in the FSW development life cycle so that the project leads understand what is required and so that there is a better chance of influencing those responsible for purchasing the parts of the test bed. Describe the following for each component.

Component #1

0. Fidelity

   - Low – generates data that may or may not be changeable in real-time via the console of the particular component
   - Medium – generates data that is responsive to commands from the ground system and from the C&DH
   - High – responds to the dynamics of the simulation (e.g. Battery State-of-Charge fluctuates with the angle of the sun on the arrays)

0. Limitations

0. Hardware maintenance agreement/understanding and contact person(s) (may be different for commercial vs special hardware)

0. Virus protection

0. System security

0. Backup plan – give the actual backup plan for each component

0. Spare parts needed

0. Software licenses needed

Component #2 (subcategories 1 – 8, just like Component #1)

]

[XXXX Mission] FSW SUSTAINING ENGINEERING TESTBED BLOCK DIAGRAM

[Insert testbed diagram here.]

6.3 HARDWARE CONFIGURATION AND CONTROL PROCESS

[Describe the method that will be used to configure and control changes to the hardware in the test bed. Nominally, hardware maintenance actions are captured via a WR or CCR.]

6.4 SYSTEM ADMINISTRATION

[Describe the system administration services that will be utilized in the maintenance of the FSTB.]

6.5 SECURITY AND PROPERTY MANAGEMENT

[Describe the security and property management guidelines that will be utilized in the maintenance of the FSTB.]

7.0 SYSTEM PATCHING CAPABILITIES

In this section, the capability of the FSW architecture to support the different types of patches is presented and evaluated. The risk presented in the Potential Risk column indicates the danger posed to the spacecraft or instrument should anything go awry with the associated type of patch.

Risk Definitions:

Low – an errant patch will simply have to be reloaded

Medium – an errant patch will cause the software to operate improperly for some period of time

High – an errant patch will cause a processor reset, instrument or spacecraft safing

7.1 PATCH TYPE DEFINITIONS

Table: Replaces a data table which is a collection of related data. The flight software has knowledge of the location of each table such that ground operators need only reference a table number (for the entire table load), or a table number and position within the table (for a partial table load). The flight software internally maintains table physical memory locations such that the ground can load and dump tables without the knowledge of where the data resides in physical memory, and no ground software or database change is required when the data is relocated due to a recompilation of the flight software. Telemetry monitoring tables and stored command tables are included in this patch type.

In-Line: Replaces FSW instructions and/or data directly in an image.

Jump-Logic-Return: Inserts a jump to a patch that returns to immediately below the jump after the patch has been executed.

Task Replacement: Uploads a patch which replaces an entire operating system task.

System Replacement: Completely replaces an FSW image.

EEPROM: Writes data to Electronically Erasable Programmable Read Only Memory (EEPROM). This data could be in many forms, including the direct modification of an image or data as described above in the other cases. Another mechanism frequently used is an EEPROM file system.

Type of Patch	Capability Exists	Size Range	Upload Time Range	Required State of the System for Patching	Potential Risk/ Operational Effects
Table					
In-Line					
Jump-Logic-Return					
Module Replacement					
System Replacement – C&DH and ACS					

Type of Patch	Capability Exists	Size Range	Upload Time Range	Required State of the System for Patching	Potential Risk/ Operational Effects
EEPROM					

7.2 UNIQUE PATCHING PROCEDURES

[State here whether or not any part of the FSW requires a patching procedure or uplink procedure that is out of the ordinary. Describe the procedure here or, if these procedures are already enumerated in another document such as a user's guide, cite the source here.]

8.0 RISKS

Characteristics of the FSW system maintenance plan that pose a risk to the spacecraft or instrument health and safety are described here along with the associated risk evaluation. The format for presenting each risk is as follows.

Risk: High, Medium, or Low. The risk rating is based on an evaluation of the likelihood the risk will pose a problem and the severity of that problem if it was to occur.

Summary: Describe the risk.

Suggested Solution: Describe a method or methods of mitigating this risk.

[List and describe each area of risk in the above format.]

APPENDIX A – FSW SUSTAINING ENGINEERING PREPARATIONS CHECKLIST

ADMINISTRATIVE

8. ☐ Sustaining engineering estimate has been completed.
8. ☐ FSW Sustaining Engineering funds have been negotiated.
8. ☐ Team members identified
   Members:
8. ☐ FSW Sustaining Engineering Team and flight operations team members have exchanged contact numbers.

CONFIGURATION MANAGEMENT

8. Will the FSW CM system transfer from the development phase? ☐ **YES** ☐ **NO**
8. ☐ The FSW CM system is in place.
8. ☐ The FSW Sustaining Engineering CCB has been established.
8. ☐ First CCB meeting was held.
8. Will the Code 582 CCR Database be used to track change and work requests? ☐ **YES** ☐ **NO**
8. ☐ If so, the choices for every field on the CCR and WR forms have been evaluated and are sufficient for this mission.
8. ☐ FSW Ground reference image has been established for every processor.
8. ☐ The launch version of the FSW is installed in the test bed. Version:
8. ☐ The launch version of the telemetry and command database is installed in the test bed.
8. Does the test bed ground system version match the control center's version (provided both are using the same ground system)? ☐ **YES** ☐ **NO**
   – Why not?

The following processes are in place and tailored for this mission.

8. ☐ Patch Development Procedure
8. ☐ CM Plan and Procedure
8. ☐ Archiving Procedure
8. ☐ CCR Process
8. ☐ Test Bed Move and Certification Process

Other procedures that are needed specifically for this mission and are in place (e.g. test bed power-up procedure).

8. ☐
8. ☐
8. ☐

8. ☐ A baseline archive of all software (FSW, simulator software, tools, compilers, etc.) and documentation to be used in the sustaining engineering phase is complete.

DOCUMENTATION

8. ☐ Write an Operations Agreement that includes all entities with which this FSW Sustaining Engineering Team will interface.
8. Will the electronic document system remain in place through the life of the mission? ☐ **YES** ☐ **NO**
8. ☐ If not, all documents needed for FSW sustaining engineering are configured elsewhere electronically.

TEST BED & TOOLS

8. ☐ All needed test bed components have been itemized.
8. ☐ All needed test bed components have been installed.
8. Will the test bed be moved from its current location? ☐ **YES** ☐ **NO**
8. ☐ Certification date:
8. ☐ New location:
8. ☐ Move date:
8. ☐ Move complete
8. ☐ Recertification Complete
8. ☐ All tools needed for sustaining engineering have been identified.
8. ☐ All tools needed for sustaining engineering have been developed.
8. ☐ Backup and restore processes and backup schedule have been established.
8. ☐ Backup and restore processes have been exercised.

8. ☐ Complete the following table:

Tool Name	**Function/Description**	**Needed?**	**Complete?**
Load File Creation	Generates Memory Load image file		
Dump to Load Convert	Converts dump image file to load image file		
Load Conversion	Converts a load image file from one format to another		
Overlay	Copies values from one file to corresponding values of another file		
Load Count	Counts the number of bytes in a load image file		
Load Append	Appends load image files together		
Table to Memory Convert	Generates a memory image from a table image		
Relocate Memory	Relocates memory data from a specified range of a file to a different memory range		
Table Maintenance Tool	Creates a user-specified table image & validates it against value & format constraints		
Memory to Table Convert	Generates a table load from load or dump memory addresses		
Formatted Table Print	Produces a formatted listing of a table		
Checksum Table Prepare	Inserts the correct checksum in a table load header		
Checksum Table Calculate	Performs a checksum of a table's contents		
FDF Table Utilities	Read FDF products and produce table loads		
Formatted File Print	Generates annotated reports of memory loads/dumps		
Formatted Memory Print	Produces a formatted listing of a memory file		
Memory Checksum	Produces checksum for a range of load or dump memory addresses		
Memory File Extract	Extracts a range of memory values from a load or dump file & creates a new file		
Dump Interpreter	Processes a dump file according to specified address ranges for tables, buffers, etc.		
File Compare	Compares two files and lists the differences		
PDB Generation	Maintains data in the Project Database		

Tool Name	Function/Description	Needed?	Complete?
Document Generator	Reads memory/table file and produces a readable/meaningful document; such as a Mode Transition Log interpretive tool.		
STOL Generator	Reads assembly & produces STOL install/remove routines		
UIF/Integration	Shells that integrate tools and provide help functions		
Development Tools	Compilers, linkers, s/w development tools		
Generate Science Data	Generates science data to input to the FSW		
Analyze Science Data	Performs analysis of science data output by the FSW in order to validate the FSW and its algorithms		

TESTING

8. ☐ End-to-end testing of the expected patching methods has been performed on every processor
8. ☐ All the FSW tables for every processor have been created, loaded to, and dumped from the FSW via the control center.
8. ☐ All the FSW table definitions have been tested.
8. ☐ A regression test set for every processor has been identified/created.

TRAINING

The FSW Sustaining Engineering Team has:
8. ☐ Built the FSW for every processor and compared it to the spacecraft image.
8. ☐ Built all of the simulator images.
8. ☐ Modified and built a new command and telemetry database.
8. ☐ Performed end-to-end testing of the expected patching methods on every processor.
8. ☐ Completed the training plan.
8. ☐ The FSW Sustaining Engineering Team has participated in at least one launch simulation.
8. ☐ The FSW Sustaining Engineering Team is familiar with the control center.

APPENDIX B – FSW SUSTAINING ENGINEERING CM

1.0 FSW SUSTAINING ENGINEERING CM ORGANIZATION

[Give the charter of the configuration control board (CCB) including a list of members.]

All work done by FSW engineers in the sustaining engineering phase shall be governed by the above-mentioned board and shall be documented as configuration change requests (CCRs) and work requests (WRs). Work requests track all work that does not result in a change to a configured item.

2.0 CONFIGURATION IDENTIFICATION

[Items that should be configured include but are not limited to FSW, software tools, software simulators, and documentation. For each item identified for configuration, list the following.

- Naming Convention:
- Versioning Scheme:
- Configured Location:
- Protection:
- Making a Change:
    - Edit Change History:
    - Build Procedure:
    - Release Procedure:
        - Who and/or What Receives the Release:
          (E.g. CSC-FSW, project server)
        - When the Release Should be Made:
        - What Exactly Shall be Archived and When:
        - Personnel to Notify Upon Release:
          (E.g. FSW Sustaining Engineering Team, Upper Management, FOT)
- Comments:]

3.0 ARCHIVING PROCESS

[Describe the method that will be used to archive the releases of the configured items or cite the existing procedure.]

4.0 SOFTWARE CONFIGURATION CONTROL

[Describe in detail the process that will be used to control all software that will be used during the sustaining engineering phase or cite the existing procedure. If there are commands that change FSW parameters, they should also be controlled.]

5.0 CCR/WR PROCESS

[Describe the process that will be used to open, track, and close configuration change requests and work requests.]

APPENDIX C – SPACECRAFT ANOMALY INVESTIGATION AND RESOLUTION PLAN EXAMPLE

1.0 INTRODUCTION

The purpose of this document is to outline a general procedure for the FSW Sustaining Engineering Team in investigating and resolving spacecraft anomalies.

2.0 ANOMALY INVESTIGATION

The FSW Sustaining Engineering Team will work in tandem with Flight Operations specialists and others to

- Acquire relevant data
- Process the data
- Analyze these data
- Consult with spacecraft systems specialists

2.1 Data Acquisition

Data relating to the affected system(s) are collected in the form of telemetry history records and computer memory dumps. In addition, all documentation regarding the affected system(s) is reviewed to assist in the analysis of data. A properly-configured simulator can also provide useful data.

2.2 Data Processing

The acquired data may require processing before analysis, by numerical means or format conversion. For example, the conversion of dumped memory into a load file can be used as input to a ground simulation of the on-board computer. In turn, the simulator output may be used to emulate an anomalous situation.

2.3 Data Analysis

Data may be analyzed numerically or graphically, against expected performance characteristics or specifications. Simulator scenarios may be adjusted depending on the outcome to better simulate the problem or situation, and the process may be repeated as necessary.

2.4 Consultation with Spacecraft Systems Specialists

In some cases, available documentation may be incomplete, but supplemented by the expertise and knowledge of systems specialists.

3.0 ANOMALY RESOLUTION

The entire spacecraft working group, after sharing the results of analysis in their areas of expertise, will be directed by the spacecraft operations manager or his/her designate towards a specific action intended to resolve the anomalous situation and return to normal operations. The FSW Team may be called upon to

- Provide operations support - e.g., review table loads, dumps of FSW, and procedures
- Develop, test, and support the installation of a flight software patch

3.1 Provide Operations Support

Recovery from anomalous situations often involves usage of rarely-used system tables, flags, and other configured flight software components. The FSW Team relies on documentation and configuration control of these systems to provide proper direction to the FOT in recovery operations.

3.2 Develop, Test, and Support Flight Software Patch Installation

In cases where a flight software patch is deemed necessary, the standards and procedures listed specifically for patch development, testing, and installation are utilized.

APPENDIX D – PATCH DELIVERY SUMMARY

1.0 PATCH IDENTIFIER

[This entry identifies the patch by stating the mission to which the patch pertains along with the software version number, CCR number, CCR title, and release/uplink date.]

Mission:
Software Version:
CCR Number:
CCR Title:
Uplink/Delivery Date:

2.0 PATCH DESCRIPTION

[This section contains all information relating to the circumstances and reasons for considering the change to the flight software. Typically, the explanation contains the following three parts, but the subsections may be merged into one section:]

2.1 Context / Background

[A brief description is given of the normal configuration or operating scenario of the hardware and/or software areas that are to be affected by this change. This is done to give the reader a context in which to understand the need for the changes made by the patch.]

2.2 Description of the Problem

[This paragraph describes the problem or the need for enhancement.]

2.3 Purpose of the Patch

[This provides a description of the desired results of this patch and of the way we wish to accomplish it. The action needed to attain this result is presented from a functional point of view, in a narrative form.]

3.0 CHANGES MADE BY THE PATCH

[This section delineates all the changes to configured items necessitated by the patch (e.g. software, documentation, simulators, tools, etc.). Existing data to be changed is specified by name, old value, and new value. If a routine or entire task is being rewritten and overlayed, a marked up listing of the assembled code could be referenced and attached in section 8 (Software Listings). If an instruction or two is being amended, then the specific change would be shown (old lines of code, new lines of code). All affected code and data modules shall be cited and any use of free space shall be explained.]

3.1 Software

3.2 Documentation

3.3 Simulators

3.4 Tools

3.5 Other

[Include any other configured item not listed above]

4.0 INSTALLING THE PATCH

[A step by step uplink procedure is given for operations personnel to follow so that they can prepare to execute the patch on board. Ideally, this procedure would be presented with the exact syntax used by the ground system to uplink the patch (i.e. STOL directives, proc names, etc.), but if the flight software analyst is not completely versed in this area (for example, Operations uses a different ground system from the FSW Testbed that is unfamiliar, an "English language" version might be used. In this case, extra care must be taken to ensure that the actions taken by the actual operations uplink procedure matches this implementation procedure. Included here would be any file names, support files, and information needed to verify that the patch has been installed correctly. All software and hardware configuration constraints should be explained (for example, uplink only at orbit night, turn off the XYZ task, disable the memory check sum protection, etc). The procedure should exactly follow the steps that were taken to install the patch at the simulation facility, thereby minimizing the chance for unexpected results. The uplink procedure must be carefully and thoroughly tested, with emphasis placed on avoiding placing the software in a compromised configuration during the patch, and minimizing the disturbance to normal operations.]

5.0 OPERATIONAL IMPACT

[Any effect that the patch will have on operations procedures, concerns, responsibilities, etc. is clearly explained in this section. If control center personnel must be aware of new or different information or the treatment thereof, this should be stated and presented directly to that group. Ripple effects to the ground system and database, command management systems, flight dynamics, science groups, flight software analysts, etc. must all be clearly explained. Also, if the patch is not intended as a permanent patch, the conditions of its uplink and removal as a temporary or contingency patch should be explained.]

6.0 REMOVING THE PATCH

[This section contains the instructions and ground system procedure names that are used to un-install the newly installed software and to recover the old software version.]

7.0 TEST RESULTS SUMMARY

[This section summarizes the acceptance test procedures and/or the actual simulation runs that were used to validate the patch. The extent of this documentation will depend on the complexity of the patch and the level of detail that is needed to demonstrate that the desired results are completely attained. Supporting material is attached when appropriate.]

ATTACHMENT A: SOURCE CODE LIST

[Electronic listings or copies of the code and data pages that are affected by the patch should be included with changes clearly marked. Note that these markings should reflect the exact changes implemented by the patch and not the logical equivalent that will be present in future system releases that incorporate the changes in line.]

ATTACHMENT B: INSTALLATION AND DE-INSTALLATION PROCEDURES

[This section contains the procedures that are used to install and remove the software changes.]